View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Helsingin yliopiston digitaalinen arkisto

CLASSIFYING OF FINITE GROUPS THROUGH SYLOW THEOREM

BY

OLUWATOSIN ISHMEAL

A MASTER'S THESIS SUBMITTED TO THE

DEPARTMENT OF MATHEMATICS AND STATISTICS,

FACULTY OF SCIENCE,

UNIVERSITY OF HELSINKI, FINLAND.

AUGUST 2017.

Dedication

This thesis is dedicated to my Mother, Adesike Olaleye and my late Father Oluwasegun Ishmeal and my late Uncle Professor F.A. Oladele.

Acknowledgment

I will like to acknowledge the support of the following people towards the successful completion of my degree either directly or indirectly;

Erik Elfving (Project Supervisor)

Professor Eero Saksman

Johanna R*ämö*

Saana Heimala

Taiwo Akinremi

Oluwaseun Adewumi

Olawale Taiwo

Okorodudu Sylvester

Abstract

The finite simple groups started attracting the interest of the mathematicians in the nineteenth century, especially once the concept of normal subgroups was introduced by Galois in 1832; differentiation between the simple and compound groups by Camille Jordan in 1870; and the theorems on subgroups of prime power order published by Ludwig Sylow in 1872. This was given in an historical form as a means of introduction. This thesis also focuses on the Sylow's theorem and their wide range of use in classifying finite groups in algebra. Groups of order 1-15 were classified using the Sylow's theorems in addition to other established results in algebra. The uniqueness and existence of such groups were also proved to the best of the writer's ability.

TABLE OF CONTENTS

Chapter 1

GENERAL INTRODUCTION

1.1 Historical Backgrounds

The evolution of finite group theory has four main roots: the theory of algebraic equations, number theory, geometrical theory, and analysis. These four theories explain the finite group theory as a whole. Therefore, the credit of finite group theory goes to these mathematicians: Joseph Louis Lagrange, Everiste Galois, Carl Friedrich Gauss, Felix Klein, Sophus Lie, and Jules Henry Poincaré.

The theory of Algebraic Equations (Classic Algebra) by Joseph Louis Lagrange:

In 1770 J. L. Lagrange wrote a paper, which is now known as the fundamental of group theory. In his paper he tried to solve a major problem of that time, the Polynomial Equations. The problem revolved around some unanswered questions as; do the roots in the Polynomial Equations exist? If yes, then how many? Are they positive or negative? And how to find

them?

Although the Babylonians were able to solve the quadratic equations in the early ages of 160 BC, as proved by the ancient writing on the Babylonian runes (a system of writing in ancient Babylon), they used the simple method of completing the squares to solve these equations. But the actual algebraic methods were developed in 1540. And yet the Quintic equations were not solved. (Kliener, 1986).

So, Lagrange set himself to the task of solving these equations. To solve these equations, he used the methods of reducing them. He reduced cubic and quartic equations into auxiliary equations and then solved them. He then attempted to resolve Polynomial equations of degree n. He did that by using his given theorem now known as The Lagrange Theorem. In this theorem, Lagrange resolved Polynomial Equations by finding the rational roots of the coefficients of a polynomial equation. He then found all the possible permutations of the rational roots and then subtracted them. In this manner, he was able to reduce the quintic functions into cubic functions. But when he applied the same method to the quintic functions, he found out the resolved equation was that of the 6^{th} degree.

Although Lagrange was unable to solve the quintic equation, he set a milestone in Algebra by finding the permutations of the roots of a polynomial function (Kliener, 1986).

Lagrange found a dead end in solving the quintic functions, but he paved way for others to explore the subject. His work was further explored by Vondermont in 1770. And then, in 1799, Paolo Ruffini attempted to prove that quintic and higher order functions are impossible to solve, and in the

process gave the concept of primitive groups.

Everiste Galois took Ruffini's work farther and found the groups of permutations of higher order functions.

Therefore, he proved that the solvability of the groups attached to the functions, make the higher order functions with radicles solvable. Galois was the first one to find the primitive groups and discovered the notion of subgroups. He also contributed to the theory of Modular Equations and Elliptical Functions. He published his paper at the age of eighteen in 1829, for which he is honored to be the first mathematician who linked group theory to field theory, which are collectively now known as Galois Theory.

Groups similar to Galois groups are called permutation groups these days. This concept was investigated by Augustine-Louis Cauchy, and was refined by Arthur Cayley in 1854.

Number theory (Carl Friedrich Gauss, 1801):

The second root to the Finite Groups theory is Number theory. This theory was presented by C. F. Gauss in his paper "Disquisitones" in 1801. In his paper he implicitly explains Abelian Groups. He explained his concepts of number which later became a part of the finite groups explained by Leopold Kroenecker.

Although, Gauss made an attempt to refine Fermat's last theorem, it was finished by Ernst Krummer, which lead to the introduction of groups describing factorization into prime numbers.

Gauss, in his paper, unintentionally established many properties of the Abelian groups. These groups appear in many forms. Such as: additive groups of integers modulo m', multiplicative groups of integers relatively

prime to modulo m', the group of equivalence classes of binary quadratic forms, and the group of n^{th} roots of unity.

Although his study is in the number theory context, but it considered the basis of modern algebra. In his study, Gauss showed that the non-zero integer modulo p, where p is prime, are all powers of a single element, in other words, the group ${Z_p}^*$ of such integers is cyclic. He also refines Fermat's theorem in his study and employs group theoretic ideas to prove his number theory.

The third root to the Finite groups theory is geometry. In 19^{th} century, geometry saw a spurt of growth. Many new concepts were given and different debates rose. Different branches of geometry came into being, such as: Algebraic Geometry, Differential Geometry, Projective Geometry etc.

Various methods of solving geometrical problems also rose, and were debated over, such as: synthetic vs analytical, metric vs projective. In the mid 19^{th} century, a problem rose of linking the geometrical classes and methods. This gave birth to the study of geometrical relations.

The study of geometrical relations studied the properties of figures invariant under transformation. Later, it became the study of transformations itself. In this, different transformations such as: circular transformations, inverse transformations etc., were discussed. Their connections were established and eventually this lead to Klein's group- theoretic synthesis of geometry. Klein's group theory brought order to geometry and is considered an implicit contribution to group theory. (Kliener, 1986)

1.2 Definitions and Concepts

1. **Operation:** In mathematics, a binary operation on a set is a calculation that combines two elements of the set (called operands) to produce another element of the set (more formally, an operation whose arity is two, and whose two domains and one codomain are (subsets of) the same set). Examples include the familiar elementary arithmetic operations of addition, subtraction, multiplication and division. Other examples are readily found in different areas of mathematics, such as vector addition, matrix multiplication and conjugation in groups.

2. **Group representations:** In the mathematical field of representation theory, **group representations** describe abstract groups in terms of linear transformations of vector spaces; in particular, they can be used to represent group elements as matrices so that the group operation can be represented by matrix multiplication. Representations of groups are important because they allow many group-theoretic problems to be reduced to problems in linear algebra, which is well understood. They are also important in physics because, for example, they describe how the symmetry group of a physical system affects the solutions of equations describing that system.

3. **Abelian Groups:** In abstract algebra, an **abelian group**, also called a **commutative group**, is a group in which the result of applying the group operation to two group elements does not depend on the order in which they are written (the axiom of commutativity). Abelian

groups generalize the arithmetic of addition of integers. They are named after Niels Henrik Abel.

4. **Algebraic structure:** In mathematics, and more specifically in abstract algebra, the term algebraic structure generally refers to a set (called carrier set or underlying set) with one or more finitary operations defined on it that satisfies a list of axioms.

5. **Axioms:** An axiom or postulate as defined in classic philosophy, is a statement (in mathematics often shown in symbolic form) that is so evident or well-established, that it is accepted without controversy or question. Thus, the axiom can be used as the premise or starting point for further reasoning or arguments, usually in logic or in mathematics. The word comes from the Greek *axioma* 'that which is thought worthy or fit' or 'that which commends itself as evident.'

6. **Symmetry:** Symmetry (from Greek *symmetria* "agreement in dimensions, due proportion, arrangement") in everyday language refers to a sense of harmonious and beautiful proportion and balance. In mathematics, "symmetry" has a more precise definition, that an object is invariant to a transformation, such as reflection but including other transforms too. Although these two meanings of "symmetry" can sometimes be told apart, they are related, so they are here discussed together. Mathematical symmetry may be observed with respect to the passage of time; as a spatial relationship; through geometric transformations such as scaling, reflection, and rotation; through other kinds of functional transformations; and as an aspect of abstract

objects, theoretic models, language, music and even knowledge itself.

7. **Lie groups**: In mathematics, a Lie group is a group that is also a differentiable manifold, with the property that the group operations are compatible with the smooth structure. Lie groups are named after Sophus Lie, who laid the foundations of the theory of continuous transformation groups.

8. **Poincaré groups:** The Poincaré group, named after Henry Poincaré (1906), was first defined by Minkowski (1908) being the group of Minkowski space-time isometries. It is a ten-generator non-abelian Lie group of fundamental importance in physics.

9. **Cosets:** In mathematics, if G is a group, and H is a subgroup of G, and g is an element of G, then

   (a) $gH = \{gh : h \in H\}$ is the left coset of H in G with respect to g, and

   (b) $Hg = \{hg : h \in H\}$ is the right coset of H in G with respect to g.

   (c) Only when H is normal will the set of right cosets and the set of left cosets of H coincide, which is one definition of normality of a subgroup. Although derived from a subgroup, cosets are not usually themselves subgroups of G, only subsets.

10. **Trivial Group:** In mathematics, a trivial group is a group consisting of a single element. All such groups are isomorphic, so one often speaks of *the* trivial group. The single element of the trivial group

is the identity element and so it is usually denoted as such: 0, 1 or e depending on the context. If the group operation is denoted $*$ then it is defined by $e * e = e$. The trivial group should not be confused with the empty set (which has no elements, and lacking an identity element, cannot be a group).

11. **Even permutation:** In algebra, an even permutation is a permutation obtainable from an even number of two elements swaps. In other words, a permutation where the permutation symbol is equal to $+1$.

12. **Dihedral group:** In group theory, a dihedral group is the group of symmetries of a regular polygon which includes the rotations and reflection of such polygon. It is denoted by D_n and has order $2n$.

13. **Generalized Dihedral group:** In group theory, the generalized dihedral group is defined for any abelian group H, as the semidirect product of H and $\mathbb{Z}_2$ with $\mathbb{Z}_2$ acting on H by inverting elements. It is denoted by $E_n(H)$ and has order $2n$.

14. **Dicyclic group:** In group theory, the dicyclic group for any integer $n > 1$ is defined as the subgroup of the unit quaternions generated by $\langle a, x | a^{2n} = 1, x^2 = a^n, x^{-1}ax = a^{-1} \rangle$. It is denoted by Dic_n and has order $4n$. The Quaternion group is the case when $n = 2$.

15. **General Affine group:** In group theory, the General affine group of any affine space over a field K is the group of all invertible affine transformations from the space into itself. It is denoted by $G(n, k)$ where $n \in \mathbb{N}$ and K is a field.

1.3 Aim and Objectives

The aim and objectives of the study are to deeply understand the concept of Finite Groups theory using the Sylow's theorems as a tool. Also to give an historical background of group theory, the terms and concepts used in the study of group theory.

Furthermore we shall look into the types and classifications of the groups. The theorems supporting the study, along with the examples that support them and the practical applications of the concept.

Chapter 2

INTRODUCTION TO GROUPS

2.1 What are groups?

In mathematics, a group is an algebraic structure consisting of a set of elements, associated with an operation that combines them together in a unique way. This combination of the set of elements help in creation of a third element. For elements to be part of a group, they have to satisfy four laws, called the group Axioms. These laws are closure, associativity, identity and invertibility. For example the set of integers, together with the addition operation is a group.

The axioms of a group, however, have a more abstract nature and have a vast application than the example listed above. They allow complex groups in abstract algebra and beyond to be handled in a flexible way while retaining their original structure.

Groups are based on the same fundamentals as symmetry. A symmetry group encodes symmetrical features of a geometrical object. Any set of

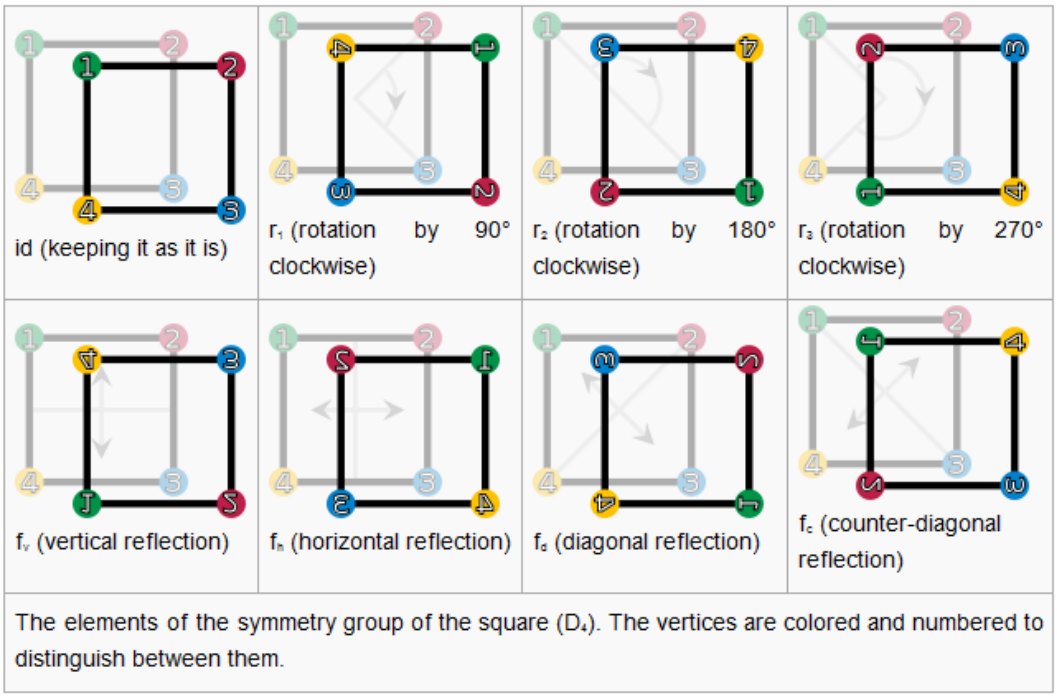
transformations made with the help of operations, leaves the structure of the object unchanged.
The examples of symmetry groups are:

- **Lie groups**: used in practical physics.
- **Point groups**: these are used to help to understand the symmetry phenomenon in molecular chemistry.
- **Poincaré groups**: these can express the physical symmetry underlying special relativity.

A practical example of a symmetry group is given as below:

Example 1.1:

Two figures in the plane are congruent if one can be changed into the other using a combination of rotations, reflections, and translations. Any figure is congruent to itself. However, some figures are congruent to themselves in more than one way, and these extra congruencies are called symmetries. A square has eight symmetries. These are:



The elements of the symmetry group of the square (D_4). The vertices are colored and numbered to distinguish between them.

Diagram source: Wikipedia.

1. the identity operation leaving everything unchanged, denoted id;

2. rotations of the square around its center by 90° clockwise, 180° clockwise, and 270° clockwise, denoted by r_1, r_2 and r_3, respectively;

3. reflections about the vertical and horizontal middle line (f_h and f_v), or through the two diagonals (f_d and f_c).

These symmetries are represented by functions. Each of these functions sends a point in the square to the corresponding point under the symmetry. For example, r_1 sends a point to its rotation 90° clockwise around the

square's center, and f_h sends a point to its reflection across the square's vertical middle line. Composing two of these symmetry functions gives another symmetry function. These symmetries determine a group called the dihedral group of degree 4 and denoted D_4. The underlying set of the group is the above set of symmetry functions, and the group operation is function composition. Two symmetries are combined by composing them as functions, that is, applying the first one to the square, and the second one to the result of the first application. The result of performing first a and then b is written symbolically *from right to left* as

$b \bullet a$ ("apply the symmetry b after performing the symmetry a").

The right-to-left notation is the same notation that is used for composition of functions.

The group table below lists the results of all such compositions possible. For example, rotating by 270° clockwise (r_3) and then reflecting horizontally (f_h) is the same as performing a reflection along the diagonal (f_d). Using the above symbols, highlighted in blue in the group table:

•	Id	r_1	r_2	r_3	f_v	f_h	f_d	f_c
id	Id	r_1	r_2	r_3	f_v	f_h	f_d	f_c
r_1	r_1	r_2	r_3	id	f_c	f_d	f_v	f_h
r_2	r_2	r_3	Id	r_1	f_h	f_v	f_c	f_d
r_3	r_3	Id	r_1	r_2	f_d	f_c	f_h	f_v
f_v	f_v	f_d	f_h	f_c	id	r_2	r_1	r_3
f_h	f_h	f_c	f_v	f_d	r_2	id	r_3	r_1
f_d	f_d	f_h	f_c	f_v	r_3	r_1	id	r_2
f_c	f_c	f_v	f_d	f_h	r_1	r_3	r_2	id

The elements id, r_1, r_2, and r_3 form a subgroup, highlighted in red (upper left region). A left and right coset of this subgroup is highlighted in green (in the last row) and yellow (last column), respectively.

Diagram source: Wikipedia.

Given this set of symmetries and the described operation, the group axioms

can be understood as follows:

1. The closure axiom demands that the composition $b \bullet a$ of any two symmetries a and b is also a symmetry. Another example for the group operation is

   $$r_3 \bullet f_h = f_c,$$

   i.e. rotating 270° clockwise after reflecting horizontally equals reflecting along the counter-diagonal (f_c). Indeed every other combination of two symmetries still gives a symmetry, as can be checked using the group table.

2. The associativity constraint deals with composing more than two symmetries: Starting with three elements a, b and c of D_4, there are two possible ways of using these three symmetries in this order to determine a symmetry of the square. One of these ways is to first compose a and b into a single symmetry, then to compose that symmetry with c. The other way is to first compose b and c, then to compose the resulting symmetry with a. The associativity condition

   $$(a \bullet b) \bullet c = a \bullet (b \bullet c)$$

   means that these two ways are the same, i.e., a product of many group elements can be simplified in any grouping. For example,
   $(f_d \bullet f_v) \bullet r_2 = f_d \bullet (f_v \bullet r_2)$ can be checked using the group table at the right

   $$(f_d \bullet f_v) \bullet r_2 = r_3 \bullet r_2 = r_1$$

which equals

$$f_d \bullet (f_v \bullet r_2) = f_d \bullet f_h = r_1.$$

While associativity is true for the symmetries of the square and addition of numbers, it is not true for all operations. For instance, subtraction of numbers is not associative: $(7 - 3) - 2 = 2$ is not the same as $7 - (3 - 2) = 6$.

3. The identity element is the symmetry id leaving everything unchanged: for any symmetry a, performing id after a (or a after id) equals a, in symbolic form,

$$id \bullet a = a,$$
$$a \bullet id = a$$

4. An inverse element undoes the transformation of some other element. Every symmetry can be undone: each of the following transformations—identity id, the reflections f_h, f_v, f_d, f_c and the 180° rotation r_2—is its own inverse, because performing it twice brings the square back to its original position. The rotations r_3 and r_1 are each other's inverses, because rotating 90° and then rotation 270° (or vice versa) yields a rotation over 360° which leaves the square unchanged. In symbols,

$$f_h \bullet f_h = id,$$
$$r_3 \bullet r_1 = r_1 \bullet r_3 = id.$$

In contrast to the group of integers above, where the order of the operation is irrelevant, it does matter in D_4 : $f_h \bullet r_1 = f_c$ but $r_1 \bullet f_h = f_d$. In other words, D_4 is not abelian, which makes the group structure more difficult than the integers introduced first.

To explore groups, mathematicians have reduced them into subgroups, quotient groups, and simple groups. In addition to their abstract properties, group theorists also study the different ways in which a group can be expressed concretely called group representations; both from a theoretical and computational point of view.

2.2 Subgroups

A subgroup can be explained as a smaller group (H), contained in a larger or parent group (G), where H contains the identity element of G, and whenever h_1 and h_2 are in H, so are $h_1 \bullet h_2$ and ${h_1}^{-1}$. Therefore, the elements of H, equipped with the group operation on G restricted to H, form a group.
The identity and the rotations constitute a subgroup $R = \{id, r_1, r_2, r_3\}$, highlighted in red in the group table above in the example: any two rotations composed are still a rotation, and a rotation can be undone by (i.e. is inverse to) the complementary rotations 270° for 90°, 180° for 180°, and 90° for 270° (note that rotation in the opposite direction is not defined). The subgroup test is a necessary and sufficient condition for a nonempty subset H of a group G to be a subgroup: it is sufficient to check that $g^{-1}h \in H$ for all elements g, $h \in H$. Knowing the subgroups is important in understanding the group as a whole.
Given any subset S of a group G, the subgroup generated by S consists of products of elements of S and their inverses. It is the smallest subgroup of G containing S. In the introductory example above, the subgroup generated by r_2 and f_v consists of these two elements, the identity element id

and $f_h = f_v \bullet r_2$. Again, this is a subgroup, because combining any two of these four elements or their inverses (which are, in this particular case, these same elements) yields an element of this subgroup.

2.3 Quotient Groups

In some situations the set of cosets of a subgroup can be endowed with a group law, giving a *quotient group* or *factor group*. For this to be possible, the subgroup has to be normal which means that H has to conicides with all its conjugates, that is $x^{-1}Hx = H \; \forall \; x \in G$. Given any normal subgroup N, the quotient group is defined by $G \; / \; N = \{gN, \, g \in G\}$, "$G$ modulo N". In fact, the operation in G/N is well-defined. (Herstein, 1975).

This set inherits a group operation (sometimes called coset multiplication, or coset addition) from the original group G: $(gN) \bullet (hN) = (gh)N$ for all g and h in G. This definition is motivated by the idea (itself an instance of general structural considerations outlined above) that the map

$G \rightarrow G \; / \; N$ that associates to any element g its coset gN be a group homomorphism, or by general abstract considerations called universal properties. The coset $eN = N$ serves as the identity in this group, and the inverse of gN in the quotient group is $(gN)^{-1} = (g^{-1})N$.

•	**R**	**U**
R	*R*	*U*
U	*U*	*R*

Group table of the quotient group D_4 / R.

The elements of the quotient group D_4 / R are R itself, which represents the identity, and $U = f_v R$. The group operation on the quotient is shown at the right. For example, $U \bullet U = f_v R \bullet f_v R = (f_v \bullet f_v) R = R$. Both the subgroup $R = \{id, r_1, r_2, r_3\}$, as well as the corresponding quotient are abelian, whereas D_4 is not abelian. Building bigger groups by smaller ones, such as D_4 from its subgroup R and the quotient D_4 / R is abstracted by a notion called semi direct product.

Quotient groups and subgroups together form a way of describing every group by its presentation: any group is the quotient of the free group over the generators of the group, quotiented by the subgroup of *relations*. The dihedral group D_4, for example, can be generated by two elements r and f (for example, $r = r_1$, the right rotation and $f = f_v$ the vertical (or any other)

reflection), which means that every symmetry of the square is a finite composition of these two symmetries or their inverses. Together with the relations,

$r^4 = f^2 = (r \bullet f)^2 = 1$,

the group is completely described. (Lang, 2002).

2.4 Simple groups

In mathematics, a simple group is a nontrivial group whose only normal subgroups are the trivial group and the group itself. A group that is not simple can be broken into two smaller groups, a normal subgroup and the quotient group, and the process can be repeated. If the group is finite, then eventually one arrives at uniquely determined simple groups by the Jordan–Hölder theorem.

2.5 Group homomorphism

Group homomorphisms are functions that preserve group structure. A function a: $G \to H$ between two groups $(G,\bullet)$ and $(H, *)$ is called a *homomorphism* if the equation

$a(g \bullet k) = a(g) * a(k)$

holds for all elements g, k in G. In other words, the result is the same when performing the group operation after or before applying the map a. This requirement ensures that $a(1_G) = 1_H$, and also $a(g)^{-1} = a(g^{-1})$ for all g in G. Thus a group homomorphism respects all the structure of G provided by

the group axioms.

2.6 Group Isomorphism

Two groups G and H are called isomorphic if there exist group homomorphisms a: $G \to H$ and b: $H \to G$, such that applying the two functions one after another in each of the two possible orders gives the identity functions of G and H. That is, $a(b(h)) = h$ and $b(a(g)) = g$ for any g in G and h in H. From an abstract point of view, isomorphic groups carry the same information. For example, proving that $g \bullet g = 1_G$ for some element g of G is equivalent to proving that $a(g) * a(g) = 1_H$, because applying a to the first equality yields the second, and applying b to the second gives back the first.

2.7 Examples and Types of Groups

The most familiar examples of groups come from elementary arithmetic. The *Integers* form a group under addition. 0 is the identity, and the inverse of an element is its negative. Another common example of a group is called the *set of Non- Zero Rational Numbers* with the group operation multiplication. In this group, the inverse is called the reciprocal. Similarly, the *Real Numbers* and the *Complex Numbers* are groups under addition, and their non- zero elements form a group under multiplication. These common examples are examples of infinite groups. There are many finite groups as well. In fact, finite groups are often more interesting than infinite groups

because they are easier to deal with.

Consider the set $\{1, -1\}$ together with the operation multiplication. It forms a group with exactly two elements. It is closed, obeys the associative property, contains the identity and, in this case, each element is its own inverse. A slightly more interesting example is the set $\{1, -1, i, -i\}$ again with the operation of multiplication.

The set of $N \times N$ *non-singular matrices* form a group under matrix multiplication. The product of two N $\times$ N nonsingular matrices is an N-by-N nonsingular matrix; matrix multiplication is associative, the set contains the identity matrix and since the matrices are non-singular they have inverses which are also non-singular. This is our first example of a *non-commutative* group as matrix multiplication does not generally commute.

Another important group is called *Euclidean group.* It consists of all the transformations of the plane which do not alter distances. A transformation of the plane takes a point (x, y) to a point $T[(x, y)]$. If the distance between the transformed version of two points is the same as the distance between the original two points, then we call the transformation an *isometry.* If two plane geometric figures are congruent then one can be transformed into the other by an isometry. This connection to the Euclidean concept of geometric congruence gives the group its name.

What is the operation in this group? Two geometric transformations can be combined into one by letting one transformation follow the other. For instance let *R180* be a rotation of 180 degrees counter-clockwise about the origin. Let *S2,5* be a shift of 2 units in the x direction and a shift of 5 units in the y direction. Then

R180*(x, y) = (-x, -y)*

and

S2,5*(x, y) = (x+2, y+5)*

If we combine these two transformations, we get a third isometry. Let

S2,5• R180

symbolize the transformation of the plane brought about by *first* performing *R180* and then **S2.5**, then

S2,5 • R180 *(x, y) = (2-x, 5-y)*

while

R180 • S2,5 *(x, y) = (-x-2, -y-5)*

This example shows that the Euclidean group is another example of a non-abelian group.

Now the composition of two isometries is an isometry (If no distances are changed by the first transformation and no distances are changed by the next transformation then no distances are changed). This satisfies the *closure* axiom. Also the "*followed by*" operation is associative. It is true that

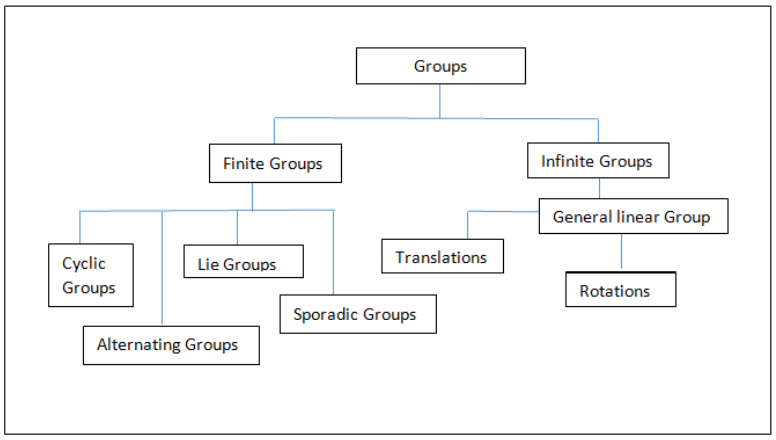
$$(A \bullet B) \bullet C = A \bullet (B \bullet C).$$

since each side of the equation is C followed by B followed by A. The identity element for isometries is the "*leave the points exactly where they are*" isometry (clearly this preserves distances). Finally, since an isometry takes any two distinct points to two other distinct points (distances must be preserved!) each isometry can be undone thus each isometry has an inverse.

A more general geometric group is the *group of similitude*. This group corresponds to the geometric notion of similar figures, figures having the same shape but different sizes. This group includes the operation of *dilation* which shrinks or stretches the plane by the same factor in all directions. A dilation $D3$ would stretch the plane by a factor of three taking *(x, y)* to *(3x,3y)*. If two figures are similar in the Euclidean definition then a *similarity* transformation changes one into the other.

A still more general group of transformations of the plane is the *affine group*. In addition to dilations the affine group includes operations which preserve straightness of lines and parallelism. They include shears and stretches of the plane in one direction. For example, any square could be transformed into any parallelogram by an affine transformation. Since these transformations are invertible, and associative we still have the group axioms satisfied.

Types of Groups:



Chapter 3

Sylow's theorems and their applications

3.1 Sylow's theorems

From abstract algebra, we know that the problem of classifying groups of every order is very difficult to deal with. Assuming though that this is not the case, then given any group G, the first thing to do to understand G is to look for subgroups H. In particular if H is a normal subgroup in G, denoted by $H \trianglelefteq G$, then one can take the quotient G/H and one can think of G as being built up from the two smaller groups H and G/H. In turn, one can then consider H, and try to break it up into smaller pieces. This is where the Sylow's theorems come into play in classification of finite groups as the theorems help break groups with large order into smaller parts. In this chapter we will consider how the Sylow's theorems are used in terms of

their application in classifying groups. We begin by giving the definitions needed to understand the concept of the Sylow's theorems.

Definition 3.1:
Let G be a non-trivial group, G is simple if it has no proper normal subgroups.

Definition 3.2:
A group whose order is power of a prime p is called a p-group. Let G be a finite group of order $n = p^k m$, where $k \in \mathbb{N}$, p is prime and p does not divide m. A subgroup H of order p^k is called a Sylow p-subgroup of G.

Remark: Simple groups can be viewed as the building blocks of any arbitrary groups and thus it is important that all finite simple groups are classified. One way of doing this is by finding normal subgroups of a group G. Lagrange's theorem leads to two implication in this respect, the first is that, in trying to proof the theorem, one key part is to use the decomposition of G into the left coset of H in G and to prove that each of that each of these cosets has the same cardinality. Secondly, it is also important from Sylow's theorems that we consider the prime factorization of order of group G. Thereafter, we can pick the prime dividing the order of G and look for normal subgroups of order of power of p.
The following theorem will give the statement of the famous Sylow's theorem and we will look at some examples about the theorems.

Theorem 3.1: SYLOW

Let G be a finite group of order $n = p^k m$, where $k \in \mathbb{N}$, p is prime and p does not divide m, then;

1. G has a subgroup of order p^k.
2. Any two Sylow p-subgroups are conjugate.
3. The number of Sylow p-subgroups is congruent to *1* modulo p, and $n_p|m$.
   (Wallace)

With the Sylow Theorems in hand, let us give two examples of this theorem.

Example 3.1:

Let the order of group G be 894348. We are interested in finding how many Sylow p-subgroup G has.

First, we need to find the prime factorization of order of G, which is $2^2 \cdot 3^3 \cdot 7^2 \cdot 13^2$. Thus, G has Sylow 2-subgroup of order 4, Sylow 3-subgroup of order 27, Sylow 7-subgroup of order 49 and Sylow 13-subgroup of order 169.

Example 3.2:

Let S_3 be the symmetry group of 3 objects. From Algebra ll, we know that the order of $S_3 = 3! = 3 \cdot 2 \cdot 1 = 6$. The subgroup $H = \{(1), (123), (132)\}$ is a normal subgroup of order 3.

Proposition 3.1:

If G is a group of order 15, then G has a normal subgroup of order 5.

Proof: To prove (3.1), we assume that we have a group G with order less than 60. Thus, assuming that $|G| = 15$. Then the prime factorization of $15 = 3 \cdot 5$. Let $p = 5$, then we know from the third Sylow theorem that the number of n_5 of Sylow 5-subgroup $\equiv 1$ mod 5 and that n_5 must divide 3.
Thus; $n_5 = 1, 6, 11, 16 \ldots$
n_5 is suppose to divide 3 and since no n_5 divides 5, then $n_5 = 1$ and there is one Sylow 5-subgroup which is, by theorem 3.3, normal in G. Therefore, G has a normal subgroup of order 5 and index 3.

Theorem 3.2:
Let G be a group of order pq, the product of two primes. Then G has a proper normal subgroup. In particular G is not simple.
For this prove of this theorem, we need an easy but useful lemma.

Lemma 3.1
Let A be a finite abelian group. Let p be a prime such that every element of A has an order which is a power of p. Then A is a p-group.
Note: The proof of this lemma is found in Wallace page 213.

Proof of theorem 3.2:
If $p = q$, then the order of the group is of the form $|G| = p^2$ and thus the group is abelian and the result holds true from the implications of lemma 3.1. But assume that $p > q$, let n_p be the number of Sylow p-subgroups.

Then we know that $n_p \equiv 1$ mod p or in other words $n_p = 1 + kp$, for some $k \in \mathbb{N}$ and n_p divides $|G|=pq$. Since n_p does not divide p, then it must divide q. Hence $k = 0$, implies that $n_p = 1$ and the Sylow p-subgroup is unique. Therefore, the Sylow p-subgroup is normal by theorem 3.3. It is a proper subgroup and thus G is not simple.

3.2 Normal Sylow subgroups

Now that the Sylow's theorem has been introduced and we have seen how it works, it is a point of interest to demonstrate the third condition on n_p in the Sylow's theorem allows us to compute n_p for several specific groups. Thus, we will see how these can be applied to group structures such as commutativity, normal subgroup and classification of simple groups of different order.

Theorem 3.3:

The condition $n_p = 1$ means that the p-Sylow subgroup is a normal subgroup.

Proof:

All p-Sylow subgroups are conjugate by Sylow 2, so $n_p = 1$ precisely when a p-Sylow subgroup of G is self-conjugate, i.e., is a normal subgroup of G.

Remark: In particular, the Sylow theorems are a tool for proving a group has a normal subgroup besides the trivial subgroup and the whole group,

because we can try to show $n_p = 1$ for some p. However, there are groups that have nontrivial normal subgroups but no nontrivial normal Sylow subgroups. This is based on the following consequence of the Sylow theorems.

Theorem 3.4:

A group G of order 1967 is not simple.

Proof:

By prime factorization, we have that $1967 = 7 \cdot 281$. Thus, the number of Sylow 7-subgroup $n_7 \equiv 1 \bmod 7$ and must divide 281 and the number of Sylow 281-subgroup $n_{281} \equiv 1 \bmod 281$ and must divide 7.

Thus $n_7 = 1, 8, 15, 21, 28, ...$ and $n_{281} = 1, 282, 563, 844, 1125....$

Therefore; both n_7 and $n_{281} = 1$. Hence, this implies that the unique Sylow 7-subgroup and Sylow 281-subgroup are normal in G. Thus G is not simple.

Theorem 3.5:

There are 48 elements of order 7 in a simple group of order 168.

Proof:

By prime factorization, we have that $|G| = 168 = 2^3 \cdot 3 \cdot 7$, and since I am interested in the element of order 7, it means that $n_7 \equiv 1 \bmod 7$ and n_7 must divide 24.

Therefore, $n_7 = 1, 8, 15, ...$ and 8 divides 24, which implies that $n_7 = 8$. Thus, there are 8 Sylow 7-subgroups but each of these subgroups contains 7 elements. By lemma 4.1, we have that $8(7 - 1) = 48$. Thus, there are 48

elements of order 7.

3.3 Commutativity properties based on $|G|$

Wallace (2012) proved that all groups of order p^2 are abelian. It is also possible to use Cauchy theorem to show that all groups of order pq with primes $p < q$ and $q \not\equiv 1 \ mod \ p$ are abelian (and in fact cyclic). We will show the relationship between abelian and cyclic groups and then continue further to use Sylow's theorems as tools to show two examples of groups with given size that are abelian.

Theorem 3.6:

Let G be a cyclic group, then G is also abelian.

Proof:

Let G be a cyclic group, by definition it means that G is generated by one generator. Let the generator be x, then if x^a and x^b are two elements of the group, for any $a, b \in \mathbb{Z}$ then;

$$x^a x^b \overset{1}{=} x^{a+b} \overset{2}{=} x^{b+a} = x^b x^a$$

This implies that G is abelian.

Note: 1. Law of additive commutativity .

2. Law of indices.

Theorem 3.7:

Let G be a group of order 207, then G is abelian.

Proof:

By prime factorization, we have that $|G| = 207 = 3^2 \cdot 23$. Let n_3 be the number of Sylow 3-subgroups and n_{23} be the number of Sylow 23-subgroups, then we know that;

$n_3 \equiv 1 \bmod 3$; $n_3|23$ and $n_{23} \equiv 1 \bmod 23$; $n_{23}|3$. This gives that $n_3 = 1$ and $n_{23} = 1$. Thus, the Sylow 3-subgroups of order 9 is of the form of 3^2, where 3 is prime, and thus implies abelian. Similarly, the Sylow 23-subgroups of order 23 is also abelian, because 23 is prime. Thus, the order of G is the direct product of the two subgroups with order 9 and 23 and this implies that G is abelian.

Theorem 3.8:

Let G be a group of order 525, then G is abelian.

Proof:

By prime factorization, we have that $|G| = 525 = 3 \cdot 5^2 \cdot 7$. Let n_3 be the number of Sylow 3-subgroups, n_5 be the number of Sylow 5-subgroups and n_7 be the number of Sylow 7-subgroups, then we know that;

$n_3 \equiv 1 \bmod 3$; $n_3|175$, $n_5 \equiv 1 \bmod 5$; $n_5|21$ and $n_7 \equiv 1 \bmod 7$; $n_7|75$.

By calculating, we get that $n_3 = 1$, $n_5 = 1$ and $n_7 = 1$. The Sylow 3-subgroup of order 3 is prime and therefore abelian. Also, Sylow 5-subgroup of order 25 is of the form 5^2, where 5 is prime and this gives that it is abelian and Sylow 7-subgroup of order 7 is prime which implies abelian and from

direct product of group, this implies that G is abelian.

Chapter 4

MORE APPLICATIONS

In the previous chapter, I have introduced the Sylow's theorem, which form a strong basis for the idea of classification of finite group, and I have applied the theorem to explain how to show whether a group is simple, has normal subgroup and is abelian. In this chapter, we will continue the application of Sylow's theorem to cyclic groups, groups of specific order (which has been chosen randomly without any special interest except to demonstrate further how the Sylow's theorem works), and non trivial normal subgroups.

4.1 Application of Sylow's theorem to characterizing cyclic groups

Theorem 4.1:

Let G be a group with prime order p, then G is cyclic.

Proof:

Let $g \in G$, where $g \neq e$. We want to show that $\langle g \rangle = G$. We know from Lagrange's theorem that any subgroup of G has order dividing p, that is either order 1 or p. The subgroup $\langle g \rangle$ contains at least two element which are g and e where $g \neq e$. Thus $\langle g \rangle = p$. Thus, this subgroup generates the whole group.

Theorem 4.2:

Let p and q be primes where $p < q$ and $q \not\equiv 1 \ mod \ p$. Then any group of size pq is cyclic.

Proof:

Let G be a group with order pq, where $p < q$ and $q \not\equiv 1 \ mod \ p$. By Cauchy's theorem, we know that G has an element a of order p and an element b of order q. Let $P = \langle a \rangle$ and $Q = \langle b \rangle$. These subgroups have size p and q and are, respectively, p-Sylow and q-Sylow subgroups of G. Using the Sylow theorems, we will show P and Q are both normal subgroups of G. But first, we are interested in finding the order of ab. To do this, we raise ab to power n. From the table of elements of $\langle ab \rangle$, we get that $\langle ab \rangle$ has elements of order pq. But we want to eliminate the possibilities of counting the same elements twice (double counting).

Suppose that $a^i b^j = a^k b^l$, then we get that $a^{(i-k)} = b^{(l-j)}$. $a^{(i-k)} \in P$ and $b^{(l-j)} \in Q$. We know that the order $a^{(i-k)} | p$ and the order $b^{(l-j)} | q$. Since p and q are coprime, then only $\{e\}$ satisfy this property. That is $a^{(i-k)} = e = b^{(l-j)}$. Thus $i = k$ and $l = j$. So, the GCD $(p, q) = 1$ and that

implies that the LCM$(p, q) = pq$. As order of G = pq, this implies that G is cyclic.

By Sylow's theorem (3), $n_p|q$ and $n_p \equiv 1 \ mod \ p$. Thus, the only choices are n_p= 1 or q. Since $q \not\equiv 1 \ mod \ p$ (by hypothesis) we must have $n_p = 1$, so P is the only p-Sylow subgroup and is thus normal in G. By Sylow's theorem (3), $n_q|p \ and \ n_q \equiv 1 \ mod \ q$. The only choices are $n_q = 1$ or p. Since $1 < p < q$, the congruence condition on n_q implies $n_q = 1$. Therefore Q is the only q-Sylow subgroup and is thus normal in G.

Remark: It is possible to show with Lagrange theorem that any group of prime order must be cyclic.

Note: For more about Cauchy Theorem, see Hungerford page 93.

Theorem 4.3: A finite group with at most one subgroup of any size is cyclic.

Proof: The argument has two steps: verify the theorem for groups of prime-power order and then use Sylow I to derive the general case from the prime-power case.

Step 1: Let $|G| = p^k$ where p is prime, $k \geq 1$, and assume G has at most one subgroup of each size. To show G is cyclic, let g be an element of G with maximal order. We want $\langle g \rangle = G$. Pick any $h \in G$, so the order of h is a power of p by Lagrange. Let g have order p^m and h have order p^n, so $n \leq m$. Then p^n divides p^m, so there is a subgroup of the cyclic group G with order p^n. (Explicitly, it is $\left\langle g^{p(m-n)} \right\rangle$.) Also $\langle h \rangle$ has order p^n, so our hypothesis that G has at most one subgroup per size implies $\langle h \rangle \subset \langle g \rangle$, so $h \in \langle g \rangle$. Therefore $G \subset \langle g \rangle$, so $\langle g \rangle = G$.

Step 2: Let G be a finite group with at most one subgroup per size. Therefore $n_p = 1$ for all primes p. For different primes p and q dividing $|G|$, the elements of the p-Sylow and q-Sylow subgroups commute with each other. Any subgroup of G has at most one subgroup of any size (otherwise G itself would have two subgroups of the same size), so by Step 1 the p-Sylow subgroup of G is cyclic. Choose a generator g_p of the p-Sylow subgroup of G. The order of g_p is the size of the p-Sylow subgroup of G. These g_p's commute as p varies, by the previous paragraph, and their orders are relatively prime, so the product of the g_p's has order equal to the product of the sizes of the Sylow subgroups of G. This product of sizes is $|G|$, so G is cyclic.

4.2 Application of Sylow's theorem to Symmetric group S_4, S_5 and Alternating group A_4, A_5

Theorem 4.4:

The groups A_4 have 3 subgroups of order 4 and 4 subgroups of order 3 and S_4 has 3 subgroups of order 8 and 4 subgroups of order 3.

Proof:

By prime factorization, we have that $|A_4| = 12 = 2^2 \cdot 3$. Let n_2 and n_3 be the number of 2-Sylow subgroups and 3-Sylow subgroups respectively. By Sylow (3), we know that $n_2 | 3$ and $n_2 \equiv 1 \bmod 2$, so $n_2 = 1$ or 3. There are

more than one transposition in A_4, thus $n_2 \neq 1$. This means that $n_2 = 3$. Also, $n_3|4$ and $n_3 \equiv 1 \bmod 3$, so $n_3 = 1$ or 4. The number of 3-cycles (abc) in A_4 is 8, and these come in inverse pairs, giving us 4 subgroups of size 3. Thus, there are 3 subgroups of order 4 and 4 subgroups of order 3 in A_4.

Next, the $|S_4| = 24 = 2^3 \cdot 3$. Let n_2 and n_3 be the number of 2-Sylow subgroups and 3-Sylow subgroups respectively. By Sylow (3), we know that $n_2|3$ and $n_2 \equiv 1 \bmod 2$, so $n_2 = 1$ or 3. There are more than one transposition in A_4, thus $n_2 \neq 1$. This means that $n_2 = 3$. Also, $n_3|8$ and $n_3 \equiv 1 \bmod 3$, so $n_3 = 1$ or 4. The number of 3-cycles (abc) in S_4 is 8, and these come in inverse pairs, giving us 4 subgroups of order 3.

Hence, both A_4 and S_4 has 4 subgroups of order 3. Individually, A_4 has 3 subgroups of order 4 and S_4 has 3 subgroups of order 8.

Theorem 4.5:

The groups A_5 and S_5 each have 10 subgroups of order 3 and 6 subgroups of order 5.

Proof:

Any element of odd order in a symmetric group is an even permutation, so the 3-Sylow and 5-Sylow subgroups of S_5 lie in A_5. Therefore, it is sufficient to focus on A_5. By prime factorization, we have that $|A_5| = 60 = 2^2 \cdot 3 \cdot 5$, the 3-Sylow subgroups have size 3 and the 5-Sylows have size 5. By Sylow (3), we know that $n_3|20$ and $n_3 \equiv 1 \bmod 3$, so $n_3 = 1, 4,$ or 10. The number of 3-cycles (abc) in A_5 is 20, and these come in inverse pairs, giving us 10 subgroups of size 3. So $n_3 = 10$. Turning to the 5-Sylows, $n_5|12$ and $n_5 \equiv$

1 mod 5, so n_5 is 1 or 6. Since A_5 has at least two subgroups of size 5 (the subgroups generated by (12345) and by (21345) are different), $n_5 > 1$ and therefore $n_5 = 6$.

4.3 Non-trivial normal subgroups

The consequences of the Sylow theorems in this section are cases where the size of G forces G to have a nontrivial normal subgroup (usually, but not always, a normal Sylow subgroup). First let's begin by introducing a lemma;

Lemma 4.1:

If G has k subgroup of order p, it has $k(p-1)$ element of order p.

Proof:

We know G has k number of subgroups, each with size p, with the identity element $\{e\}$ belonging to each of these subgroups, that gives $k(p-1)$ number of element. Next, we have to eliminated the possibilities that no other element belong to the intersection of two different subgroups of G. So, if H and K are two different subgroups of G, then we claim that $H \cap K = \{e\}$. Lagrange's theorem can help in this part. We know that if $H \cap K \neq \{e\}$, say $H \cap K = l$, this implies that l is a generator for H and K and that means that $H = K$. Since p is a prime, it necessarily generates H and K. Thus, no other element belongs to $H \cap K$ except $\{e\}$. Therefore, G has $k(p-1)$ elements of order p.

Theorem 4.5:

Let $|G| = 20$ or 100, then G has a normal 5-Sylow subgroup.

Proof:

Let $|G| = 20$, then by prime factorization, we have that $20 = 2^2 \cdot 5$. By Sylow (3), $n_5|4$ and $n_5 \equiv 1 \ mod \ 5$. Thus $n_5 = 1$. Also, let $|G| = 100$, by prime factorization, we have that $100 = 2^2 \cdot 5^2$. From here the proof follows similarly.

Theorem 4.6: Let $|G| = 12$ then G has a normal 2-Sylow or 3-Sylow subgroup.

Proof:

By Sylow (3), $n_2|3$, so $n_2 = 1$ or 3. Also $n_3|4$ and $n_3 \equiv 1 \ mod \ 3$, so $n_3 = 1$ or 4. We want to show $n_2 = 1$ or $n_3 = 1$.

Assume $n_3 \neq 1$, so $n_3 = 4$. Since the 3-Sylows have size 3, Lemma 4.1 says G has $n_3 \cdot 2 = 8$ elements of order 3. The number of remaining elements is $12\text{-}8 = 4$. A 2-Sylow subgroup has size 4, and thus fills up the remaining elements. Therefore $n_2 = 1$. For example, A_4 has $n_2 = 1$ and $n_3 = 4$, while D_6 has $n_2 = 3$ and $n_3 = 1$.

4.4 Application to classifying finite groups

Next, we will apply all the concepts that has been developed to classifying groups with finite order from 1 to 25 and show the uniqueness and existence of such groups. The classification will be arranged first in terms of prime order which are the simpler ones and similar orders that behave the same way will follow. The group of order 1 is the identity element and has only one finite group, this is trivial so we will not talk about it.

Theorem 4.7: Let G be a group of prime order p, then up to isomorphism, there is only one group of finite order with order p.

Proof:

From Algebra ll and theorem 4.1, we know that a group of prime order is cyclic and thus the only possibility is the group $\mathbb{Z}_p$. This confirms the uniqueness of $\mathbb{Z}_p$, also the group $\mathbb{Z}_n$ is a well known from Algebra ll and in mathematics at large. Thus, this takes care of finite groups with order 2,3,5,7,11,13.

Theorem 4.8: Let G be any group with order 4, then up to isomorphism, there are exaclty 2 groups of order 4 which are $\mathbb{Z}_4$ and $\mathbb{Z}_2 \bigoplus \mathbb{Z}_2$.

Proof:

To prove the uniqueness of this groups, we will manually write out the elements using the multiplication table. The idea is to multiply the elements

together, at some point there will be nothing to multiply unless we assume that given any element $a \in \mathbb{Z}_4$, then $a \cdot a = b$ or $a \cdot a = e$. Doing this, we will get a table that looks like that $\mathbb{Z}_4$ and $\mathbb{Z}_2 \bigoplus \mathbb{Z}_2$. This proves that there cannot be any other possibilities except this two. So we get a table that looks like this for $a \cdot a = e$:

·	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

and for $a \cdot a = b$.

·	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

For existence, both groups $\mathbb{Z}_4$ and $\mathbb{Z}_2 \bigoplus \mathbb{Z}_2$ exists and well known.

Theorem 4.9: Let p and q be primes such that $p > q$. If $q \nmid (p-1)$, then every group of order pq is isomorphic to the cyclic group $\mathbb{Z}_{pq}$. If $q|p-1$, then up to isomorphism, there are exactly two distinct groups of order pq: the cyclic group $\mathbb{Z}_{pq}$ and a non-abelian group group K generated by elements c and d such that $|c| = p$ and $|d| = q$ and $dc = c^s d$ where $s \not\equiv 1(mod\ p)$ and $s^q \equiv 1(mod\ p)$.

Proof:

First, given a group G of order pq, we know that by Cauchy theorem there exists elements $a, b \in G$ with order p, q respectively, that is, $|a| = p$ and $|b| = q$. Let $|G| = pq$, and $p > q$, by Sylow theorem, we know that the number of Sylow p-subgroups n_p is congruent to 1 mod p and divides q, this means that $n_p = 1, 1 + p, 1 + 2p$ and should divide q. But since $p > q$, then $n_p = 1$, this means that n_p is a normal subgroup of G. Thus G has a subgroup of order p which is S. Let $\langle a \rangle = S \subset G$. Now, consider the factor group G/S with the coset bS that has order q. This gives that the factor group $|G/S| = q$. Thus G/S is cyclic and bS is its generator, so we have that $G/S = \langle bS \rangle$ and $S = \langle a \rangle$. Therefore, every element of G can be written in the form $b^i a^j$ because since $\langle a \rangle$ and $\langle bS \rangle$ are subsets of G and G is generated by $a, b \in G$, then by I.2.8 (Hungerford) every element of G is a finite product $a^{m_1} b^{m_2} a^{m_3} b^{m_4} \cdots b^{m_k}$ for $m_i \in \mathbb{Z}$ and by repeated use of I.6.13 (Hungerford), any such product may be written in the form $a^i b^j$ with $0 \leq i < n$ and $j = 0, 1$.

Second, we know that the number of Sylow q-subgroups is congruent to $1(mod\ q)$ and divides pq. Hence, it is 1 or p.

Case 1: If it is 1, (then it means that $q \nmid p - 1$), then $\langle b \rangle$ is normal in G by theorem 3.3. Next, we have that $\langle a \rangle \trianglelefteq G$ and $\langle b \rangle \trianglelefteq G$. Combining theorem I.4.6 (Hungerford) and the fact that finite intersection of of subgroup of a group G is a subgroup of G, we get that $\langle a \rangle \cap \langle b \rangle = \langle e \rangle$. Thus from theorem I.8.6 (Hungerford), $G \cong \langle a \rangle \times \langle b \rangle$. Next, we have to show that since $\langle a \rangle$ and $\langle b \rangle$ are cyclic, then their product is cyclic. We know that $|\langle a \rangle| \times |\langle b \rangle| = |\langle a \rangle|\,|\langle b \rangle| = pq$. So, $\langle a \rangle \times \langle b \rangle$ is cyclic if and only if

there is an element of order pq in $\langle a\rangle \times \langle b\rangle$ and the condition for that is $\gcd(|\langle a\rangle|, |\langle b\rangle|) = 1$, which is true in this case since $p > q$. On the other hand, if the condition is false, that is, $\gcd(|\langle a\rangle|, |\langle b\rangle|) > 1$, then it implies that $\text{lcm}(|\langle a\rangle|, |\langle b\rangle|) < pq$. Thus, $\langle a\rangle \times \langle b\rangle$ has all elements of order less than pq and this gives that $\langle a\rangle \times \langle b\rangle$ is noncyclic. Finally, we know that finite cyclic group is isomorphic to Z_m and as such $G = \langle a\rangle \times \langle b\rangle \cong \mathbb{Z}_p \bigoplus \mathbb{Z}_q \cong \mathbb{Z}_{pq}$.

Case 2: If the number is p (which can occur in the case $p|q-1$), since $\langle a\rangle \trianglelefteq G$, and by theorem I.3.4(v) (Hungerford), it implies that $bab^{-1} = a^r$ and $r \not\equiv 1(mod\ p)$. (Otherwise G would be abelian, and hence have a unique sylow q-subgroup). Since $bab^{-1} = a^r$, it follows by induction that, $b^iab^{-i} = a^{r^i}$. In particular for $i = q$, $a = a^{r^q}$ which implies that $r^q \equiv 1(mod\ p)$.

Third, we need to show that if $q|p-1$ and G is the non-abelian group, then G is isomorphic to K. We know from number theory that $X^q \equiv 1(mod\ p$ has exactly q distint solution modulo p. If r is a solution and k is the least positive integer such that $r^k \equiv 1(mod\ p)$, then $k|q$. (Shockley, theorem 8). In this case, $r \not\equiv 1(mod\ p)$ whence $k = q$. It follows that $1, r, r^2, \cdots, r^{q-1}$ are all the distinct solutions modulo p of $X^q \equiv 1(mod\ p)$. Consequently, $s \equiv r^t(mod\ p)$ for some $t(1 \leqslant t \leqslant q-1)$. If $b_1 = b^t$, then $|b_1| = q$ and this shows that $G = \langle a, b_1\rangle$, that is, every element of G can be written in the form $b_1^i a^j$ (same reason as above) and that $|a| = p$ and that $b_1ab^{-1} = b^tab^{-t} = a^{rt} = a^s$. Therefore $b_1a = a^sb_1$.

To finish the proof, we need to verify that the map $G \to K$ given as $a \mapsto c$ and $b_1 \mapsto d$ is an isomorphism. Since $G = \langle a, b_1\rangle$ and $K = \langle c, d\rangle$, then G and K has the same order pq, thus by definition we have that:

$G = \{a^0b_1^0, a^1b_1^1, a^2b_1^2, \cdots a^{i-1}b_1^{j-1}\}$ and $K = \{c^0d^0, c^1d^1, c^2d^2, \cdots, c^{i-1}d^{j-1}\}$. Thus, if we set up a bijection $\phi : G \to K$ defined by $\phi(a^ib_1^j) = c^id^j$. Then, we need to show that ϕ is an isomorphism. First, $\phi(a^ib_1^j) = c^id^j$ holds for all $n \in \mathbb{Z}$. Let $n \in \mathbb{Z}$, by the division theorem, we can write $n = kt + r; 0 \leqslant r < k$, which gives $n - r = kt$ and this implies that $k|(n-r)$. Thus, $a^nb_1^r = a^rb_1^n; c^nd^r = c^rd^n$. Therefore, $\phi(a^nb_1^r) = \phi(a^rb_1^n) = c^rd^n = c^nd^r$. Next, we need to prove that ϕ is an homomorphism. Let elements $x, y \in G$, since $G = \langle a, b_1\rangle$, it follows that there exists $m, n \in \mathbb{Z}$ such that $x = (ab_1)^m$ and $y = (ab_1)^n$. Then; $\phi(x, y) = \phi((ab_1)^m(ab_1)^n) = \phi((ab_1)^{m+n}) = (cd)^{m+n} = (cd)^m(cd)^n = \phi(ab_1)^m\phi(ab_1)^n = \phi(x)\phi(y)$. Therefore, ϕ is an homomorphism. Also, since ϕ is bijective, then ϕ is an isomorphism from $G \to K$. Thus, $G \cong K$ and that completes the proof. For the existence of the non-abelian group K, see (Shockley, 67 corollary 6.1).

Theorem 4.10: If p is an odd prime, then every group of order $2p$ is isomorphic either to the cyclic group Z_{2p} or the dihedral group D_p.

Proof:

Applying theorem 4.9 with $q = 2$. If G is not cyclic, the conditions on s from theorem 4.9 implies that $s \equiv -1(mod\ p)$. Hence $G = \langle c, d\rangle, |d| = 2, |c| = p$ and $dc = c^{-1}d$. Thus by theorem I.6.13 (Hungerford), $G \cong D_p$.

Theorems 4.9 and 4.10 takes care of the groups of order 6, 10, 14 and 15.

Theorem 4.11: Let G be a group of order p^2 where p is prime, then up to

isomorphism, there exist 2 groups of finite order which are the cyclic group $\mathbb{Z}_{p^2}$ and a non-cyclic group which is the direct product of $\mathbb{Z}_p \bigoplus \mathbb{Z}_p$.

Proof:

To prove the uniqueness, we will first prove that all groups of order p^2 are abelian. Let G be a group and let $Z(G)$ be the center of the group, from algebra ll, we know that the center of a group is a subgroup of that group, this implies that $Z(G)$ is a subgroup of G. Next, we need to find the order of $Z(G)$, we know that the group G has order p^2, and from Lagrange, since $Z(G)$ is a subgroup of G, then $|Z(G)|$ should divide $|G|$. But $|G| = p^2$ and p is prime, that leaves us with only 3 cases, that is, 1, p, p^2.

Case 1: When $|Z(G)| = 1$. This case is impossible as the center of a group $|Z(G)| \neq 1$. (Corollary Il.5.4, Hungerford).

Case 2: When $|Z(G)| = p$. Then we have by the definition of index of a subgroup that;

$$\begin{aligned} |G/Z(G)| &= [G : Z(G)] \\ &= |G|/|Z(G)| \\ &= p^2/p \\ &= p. \end{aligned}$$

This implies that $G/Z(G)$ is non-trivial and has prime order and we know also from algebra ll that a group of prime order is cyclic, and as such $G/Z(G)$ is a cyclic group. But since $|G| \neq |Z(G)|$, then G cannot be abelian.

Case 3: When $|Z(G)| = p^2$. This gives that both G and $Z(G)$ have the same order p^2 and thus $G = Z(G)$, therefore G is abelian.

Establishing that G is abelian, the theorem of finitely generated abelian group together with theorem II.2.1 (Hungerford) proves that every finitely generated abelian group G is isomorphic to a finite direct sum of cyclic groups in which the finite cyclic summands are of order $m_1, m_2, \cdots, m_t$ where $m_1 > 1$ and $m_1|m_2| \cdots |m_t$. This gives that $G \cong Z_{m_1} \bigoplus Z_{m_2} \bigoplus \cdots \bigoplus Z_{m_t}$. For groups with order $9 = 3^2$, this gives exactly 2 finite order group up to isomorphism which are $\mathbb{Z}_9$ and $\mathbb{Z}_3 \bigoplus \mathbb{Z}_3$.

Theorem 4.12: Let G be a group of order pq where p, q are prime such that $p < q$ and $q \not\equiv 1(modp)$, then up to isomorphism, there exist only one group of order pq.

Proof:

To prove the uniqueness we will use the group of order 15 because this is the smallest order group and the only group in the order that is been considered in this thesis that exhibit these properties. Continued from proposition 3.1, since the condition $n_5 = 1$, together with theorem 3.3 and theorem 4.2, we can conclude that there exist a normal subgroup in G and thus G is cyclic. Thus there exists only one group of finite order of order 15 which is $\mathbb{Z}_{15}$. This takes care of the finite group of order 15.

Theorem 4.13: Let G be a group of order 8, then up to isomorphism there are exactly five groups of order 8.

Proof:

To prove the uniqueness of this order, we will start from theorem II.2.1

(Hungerford), we know that the condition for any abelian group G to be isomorphic to $Z_{m_1} \bigoplus Z_{m_2} \bigoplus \cdots \bigoplus Z_{m_t}$ is that the summands $m_1 > 1$ and $m_1|m_2| \cdots |m_t$. If we write $8 = 2 \cdot 2 \cdot 2 = 2 \cdot 4$. Thus, we have 3 cases to consider:

Case 1: $m_1 = 2, m_2 = 2, m_3 = 2$. Since $m_1|m_2|m_3$ and $m_1 > 1$, then, we have that $G \cong \mathbb{Z}_2 \bigoplus \mathbb{Z}_2 \bigoplus \mathbb{Z}_2$.

Case 2: $m_1 = 2, m_2 = 4$. Also, $m_1|m_2$, and $m > 1$, then, we have that $G \cong \mathbb{Z}_2 \bigoplus \mathbb{Z}_4$.

Case 3: We have that $G \cong \mathbb{Z}_8$.

Next, proposition II.6.3 (Hungerford), say that 'there are up to isomorphism, exactly two distinct non-abelian groups of order 8: the quaternion group Q_8 and the dihedral group D_4, so we will try to prove the existence of these groups and show that they are non-isomorphic.

First we will try to show that $Q_8 \ncong D_4$. We will do this by counting the number of elements of both groups. We notice that Q_8 has only one element of order 2 while D_4 has five elements of order 2 and this shows that $Q_8 \ncong D_4$. To prove the existence: Let G be a non-abelian group of order 8, we know that G cannot contain an element of order 8 or have every nonidentity element of order 2, since If $g^2 = 1$ for all $g \in G$, then G is abelian, so some $a \in G$ must have order 4. The subgroup $\langle a \rangle$ of index 2 is normal in G. Therefore, choosing $b \in \langle a \rangle$, since $\langle a \rangle$ is normal it means that $bab^{-1} \in \langle a \rangle$, we get that; $bab^{-1} \in \{1, a, a^2, a^3\}$, and since the non-identity elements in G has order 2 or order 4, then bab^{-1} must has order 4 (if the order is 2, then it is abelian and this case is non-abelian), $bab^{-1} = a$ or $bab^{-1} = a^3 = a^{-1}$. The case $bab^{-1} = a$ is not possible since G is non-abelian, so a and b do not

commute. Therefore, $bab^{-1} = a^{-1}$. It follows that every element of G can be written in the form $b^i a^j$ as in theorem 4.9. Next, we know that the group $|G/\langle a\rangle| = 2$, so $b^2 \in \langle a\rangle$ means that $b^2 \in \{1, a, a^2, a^3\}$, since b has order 2 or 4, b^2 has order 1 or 2. Thus, $b^2 = a^2$ or $b^2 = 1$. Hence, $G = \langle a, b\rangle$ where either $a^4 = 1, b^2 = 1, bab^{-1} = b^{-1}$ or $a^4 = 1, b^2 = a^2, bab^{-1} = b^{-1}$. The case $a^4 = 1, b^2 = 1, bab^{-1} = b^{-1}$ or $ba = a^{-1}b$ by I.6.13 (Hungerford) gives that $G \cong D_4$ and the case $a^4 = 1, b^2 = a^2, bab^{-1} = b^{-1}$ or $ba = a^{-1}b$ by I.4.14 (Hungerford) gives that $G \cong Q_8$.

Theorem 4.14: Let G be a group of order 12, then up to isomorphism, there are exactly five groups of finite order.

Proof:

To prove the uniqueness, we will also start from theorem II.2.1, the condition for G to be isomorphic cyclic group $Z_{m_1} \bigoplus Z_{m_2} \bigoplus \cdots \bigoplus Z_{m_t}$ is assumed known. If we write $12 = 2 \cdot 6 = 3 \cdot 4$, we see that only $12 = 2 \cdot 6$ satisfies the conditions. Thus we have 2 cases to consider.

Case 1: $m_1 = 2, m_2 = 6$. Since $m_1 | m_2$ and $m_1 > 1$, then, we have that $G \cong \mathbb{Z}_2 \bigoplus \mathbb{Z}_6$.

Case 2: We know that G is isomophic to the cartesian product of its summand, that is, $2 \times 6 = 12$, thus $G \cong \mathbb{Z}_{12}$.

Next, proposition II.6.4 (Hungerford), say that there are up to isomorphism, exactly three distinct non-abelian groups of order 12: the dihedral group D_6, the alternating group A_4, and a group T generated by elements a, b such that $|a| = 6, b^2 = a^3$ and $ba = a^{-1}b$. To prove this, we will start by

verifying that there is a group T of order 12 and that no two of T, A_4, D_6 are isomorphic. To verify T, let T be a non-abelian group of order 12. The non-identity elements of T have order 2 or 6. If $g^2 = 1$, for all $g \in T$, then T is abelian, so some $a \in T$ must have order 6 which is isomorphic to S_3, that is, the symmetry group of 3 elements. Since $\langle a \rangle$ has 2 index in T, then $\langle a \rangle$ is normal in T. Therefore, choosing $a \in \langle a \rangle$, we get that $bab^{-1} \in \langle a \rangle$ which gives $bab^{-1} \in \{1, a, a^2, a^3, a^4, a^5\}$. Since bab^{-1} has order 6, then $bab^{-1} = a$ or $bab^{-1} = a^5 = a^{=1}$. Since T is non-abelian then the first option is not possible as a and b do not commute. Therefore, we have that $bab^{-1} = a^{-1}$. Next, the group $T/\langle a \rangle$ has order 2, so $b^2 \in \langle a \rangle$ gives $b^2 \in \{1, a, a^2, a^3, a^4, a^5\}$. Since b has order 2 or 6, b^2 has order 1 or 3. Thus, $b^2 = 1$ or $b^2 = a^3$. Thus we have that $T = \langle a, b \rangle$, where $a^6 = 1, b^2 = a^3, bab^{-1} = a^{-1}$ or $ba = a^{-1}b$. This gives the group T. Also, $a^6 = 1, b^2 = 1, bab^{-1} = a^{-1}$ or $ba = a^{-1}b$ gives the group D_6.

Next, we need to prove that no two of T, A_4, D_6 are isomorphic. If we choose A_4, D_6 and the count the order of the elements in the groups, the 60-degree rotation in D_6 has order 6 but no element in the group A_4 has order 6. In fact, no element in the group S_4 has order 6. Thus, $D_6 \ncong A_4$. Next, if G is non-abelian of order 12, then, by sylow theorem, we know that G will have Sylow 3-subgroup of G. Let's call this P. Then $|P| = 3, |G|/|P| = 4$. By Proposition II.4.8 (Hungerford), there is a homomorphism $f : G \to S_4$ whose kernel K is contained in P, whence $K = P$ or $\{e\}$. If $K = \{e\}, f$ is a monomorphism and G is isomorphic to a subgroup of order 12 of S_4, which must be $A4$ by theorem I.6.8 (Hungerford). Otherwise $K = P$ and P is normal in G. In this case P is the unique Sylow 3-subgroup. Hence G

contains only two elements of order 3, assume that c is one of these, then, $[G : C_G(c)] = 1$ or 2, since $[G : C_G(c)]$ is the number of conjugates of c and every conjugate of c has order 3. Hence $C_G(c)$ is a group of order 12 or 6. In either case there is a second element $d \in C_G(c)$ of order 2 by Cauchy's theorem.

Thus, all the finite groups of order 12 are $\mathbb{Z}_2 \bigoplus \mathbb{Z}_6$, Z_{12}, T, D_6 and A_4.

All groups which have been classified in this thesis are given in the table below:

Order of group	Number of distinct group
1	1
2	1
3	1
4	2
5	1
6	2
7	1
8	5
9	2
10	2
11	1
12	5
13	1
14	2
15	1

4.5 Conclusion and Recommendation

The group theory is a very vast field of mathematics. The generalization that the group theory framework provides is so powerful that the understanding of so many different parts of mathematics is hard to imagine at first. In this thesis, the concept of group theory was revisited. The importance of the Sylow's theorems were established and together with some

established results in group theory has helped in classifying finite groups. We have also classified finite groups in terms of being simple, normal, cyclic and abelian. It is recommended that further works can be done by using other aspect of group theory in classifying finite groups and also in determining the distinct groups of larger numbers.

References

Andruskiewitsch, N., & Schneider, H. J. (2010). On the classification of finite-dimensional pointed Hopf algebras. Annals of Mathematics, 375-417.

Barut, A. O., & Raczka, R. (1986). Theory of group representations and applications (Vol. 2). Singapore: World Scientific.

Conrad K. Consequences of the Sylow Theorems.
available at http://www.math.uconn.edu/kconrad/blurbs/grouptheory/Sylowapp.pdf

Conrad K. Consequences of the Cauchy Theorems.
available at http://www.math.uconn.edu/ kconrad/blurbs/grouptheory/cauchyapp.pdf

Fang, J. (1963). Abstract algebra. Schaum Publishing company.

Foote, R. (2007). Mathematics and complex systems. Science, 318(5849), 410-412.

Gallian, J. (2016). Contemporary abstract algebra. Cengage Learning Publisher.

Gilmore, R. (2012). 'Lie groups, Lie algebras, and some of their applications'. Courier Corporation.

Gorenstein, D. (2013). Finite simple groups: An introduction to their classification. Springer Science & Business Media.

Herstein, I.N. (1975). Topics in Algebra. John Wiley & Sons.

Hungerford, T. W. (1980). Algebra, Graduate text in Mathematics. Volume 73 of Graduate Texts in Mathematics.

Idelhaj, A. (2016). The Sylow Theorems and their applications. available at http://math.uchicago.edu/ may/REU2016/REUPapers/Idelhaj.pdf

Jungnickel, D. (1992). On the Uniqueness of the Cyclic Group of Order n. The American Mathematical Monthly, Vol. 99, No. 6 (Jun. - Jul., 1992), pp. 545-547.

Kleiner, I. (1986). The evolution of group theory: A brief survey. Mathematics Magazine, 59(4), 195-215.

Mckernan, J. Sylow's theorem and Applications, http://math.mit.edu/ mckernan/Teaching/12-13/Spring/18.703/l_13.pdf.

Lang, S. (2002). Algebra, Graduate Text in Mathematics. Revised third edition. New York. Springer-Verlag. Shockley, J. E. (1967). Introduction to Number Theory. New York: Holt, Rinehart and Winston, Inc.

Solomon, R. (2001). A brief history of the classification of the finite simple groups. Bulletin of the American Mathematical Society, 38(3), 315-352.

Upadhyay, S.K., & Kumar, S.D. (2011). Existence of a unique group of finite order. arXiv preprint arXiv:1104.3831.

Wallace, D. A. (2012). Groups, rings and fields. Springer Science & Business Media.

Wilson, R. (2009). The finite simple groups (Vol. 251). Springer Science & Business Media.